UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/448,154	11/24/1999	PAUL S. GERMSCHEID	33012/274/10	4721

7590 03/25/2004

CHARLES A JOHNSON
UNISYS CORPORATION
LAW DEPARTMENT M S 4773
2470 HIGHCREST ROAD
ROSEVILLE, MN 55113

EXAMINER	
WASSUM, LUKE S	
ART UNIT	**PAPER NUMBER**
2177	

DATE MAILED: 03/25/2004

16

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/448,154	GERMSCHEID ET AL.	
	Examiner	Art Unit	
	Luke S. Wassum	2177	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 April 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9 February 2004 has been entered.

Response to Preliminary Amendment

2. An Applicants' preliminary amendment, filed 9 February 2004, has been received, entered into the record, and considered.

3. As a result of the amendment, claims 1, 3, 6-8, 11-13 and 18 have been amended. Claims 1-20 remain pending in the application.

Specification

4. In view of the Applicant's extensive discussion of the examiner's objection to the specification, the examiner withdraws the pending objection to the specification.

5. The disclosure is objected to because of the following informalities:

On replacement page 34, submitted as part of Amendment E, filed 8 December 2003, the cited application serial number should be 09/188649, not 09/188549.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 1-20 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

8. Regarding claims 1, 6, 11 and 16, the claim limitations of the independent claims regarding the use of a site specific security profile in permitting access to secure data in a database without requiring the transfer of a user identifier via a publicly accessible digital data communications network are discussed in the Summary of the Invention, pages 7-9. However, the details of the use of the site specific security profile is not disclosed in the Detailed Description of the Preferred Embodiments, and in fact the section of the Detailed Description concerning the operation of security profiles discloses a mechanism whereby a user submits a service request which results in the execution of a command language script with associated security profile which requires the user to submit a UserID over the World Wide Web in order for the execution of the script to proceed. This disclosure is inconsistent with the claim language. The lack of a detailed disclosure of the claimed invention renders the invention non-enabled.

9. Dependent claims 2-5, 7-10, 12-15 and 17-20 are rejected since they incorporate the deficiencies of their respective independent claims.

10. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. Claims 1-20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The claim language is inconsistent with the disclosure of the invention. This inconsistency renders the claims indefinite, in accordance with MPEP § 2173.03[R-1]:

> "Although the terms of a claim may appear to be definite, inconsistency with the specification disclosure or prior art teachings may make an otherwise definite claim take on an unreasonable degree of uncertainty. In re Cohn, 438 F.2d 989, 169 USPQ 95 (CCPA 1971); In re Hammack, 427 F.2d 1378, 166 USPQ 204 (CCPA 1970). In Cohn, the claim was directed to a process of treating a surface with a corroding solution until the metallic appearance is supplanted by an "opaque" appearance. Noting that no claim may be read apart from and independent of the supporting disclosure on which it is based, the court found that the description, definitions and examples set forth in the specification relating to the appearance of the surface after treatment were inherently inconsistent and rendered the claim indefinite."

12. Specifically, independent claims 1, 6, 11 and 16 contain the limitations that (1) access to secure data is requested by a user, and (2) access to the secure data is granted without transfer of a user identifier uniquely identifying the user via a publicly accessible digital communication network.

This is inconsistent with the teaching of the specification at pages 33-34, where it is taught that if a security profile is not associated with a requested service request, the service request is carried out, but if a security profile is associated with a requested service request, then

> "**service handler 332 requests the user to provide a user-id via** path 330, Cool ICE object 322, and **world wide web path** 312. **Service handler 332 awaits a response via world wide web** path 308, Cool ICE object 322 and path 326. **Service handler 332 compares the user-id received** to the security profile stored with the command language script. If the user matches the security profile, access is granted and service handler 322 proceeds as described above."

The plain implication is that if secure data is requested (assuming that an associated security profile indicates the presence of secure data), then **the user** is requested to provide a user-id, and this user-id is transmitted to the server via the world wide web. This is contrary to the claim language whereby access to secure data is granted without the transmission of user identification information over a publicly accessible digital data communications network.

13. Dependent claims 2-5, 7-10, 12-15 and 17-20 are rejected since they incorporate the deficiencies of their respective independent claims.

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. The factual inquiries set forth in *Graham* v. *John Deere Co*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

16. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

17. Claims 1-4, 6-8, 11-14 and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **Yoshimoto** (U.S. Patent 6,237,023) in view of **De Capitani di Vimercati et al.** ("Access Control in Federated Systems").

18. Regarding claim 1, **Garrison** teaches a data processing environment having a user with a user identifier which uniquely identifies said user at a terminal at a particular site which generates a service request requesting access to secure data responsively coupled via a publicly accessible digital data communication network to a database management system having at least one database containing said secure data as claimed, comprising a security profile whereby said database management system permits said terminal to access said at least one database (see col. 4, lines 1-32; see also col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

Garrison does not explicitly teach a data processing environment wherein the security profile is site-specific.

Yoshimoto, however, teaches a data processing environment wherein the security profile is site-specific (see Abstract; see also col. 1, line 63 through col. 2, line 6).

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a site-specific security profile, since this would allow the level of access granted to a user to be based in part on the security of the specific terminal or location from which the access request is generated, thus inhibiting illegitimate access from a terminal having poor security (see **Yoshimoto**, col. 6, lines 15-21).

Neither **Garrison** nor **Yoshimoto** explicitly teaches a data processing environment wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network.

De Capitani di Vimercati et al., however, teaches a data processing environment wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the three references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **Yoshimoto**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network, since it is necessary to protect all information transferred over the global communication network (see **Capitani di Vimercati et al.**, page 93, col. 2, second to last paragraph).

19. Regarding claim 6, **Garrison** teaches an apparatus as claimed, comprising:

a) a terminal located at a particular location (see col. 4, lines 1-32) having a user with a user identifier which identifies said user (see col. 6, line 60 through col. 7, line 13);

b) a database management system having access to a database responsively coupled to said user terminal via a publicly accessible digital data communication network (see col. 4, lines 1-32); and

c) a security profile generated by said database management system whereby said database management system provides access to a particular secure portion of said database corresponding to said security profile (see col. 7, line 50 through col. 8, line 37).

Garrison does not explicitly teach an apparatus wherein the security profile is site-specific.

Yoshimoto, however, teaches an apparatus wherein the security profile is site-specific (see Abstract; see also col. 1, line 63 through col. 2, line 6).

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a site-specific security profile, since this would allow the level of access granted to a user to be based in part on the security of the specific terminal or location from which the access request is generated, thus inhibiting illegitimate access from a terminal having poor security (see **Yoshimoto**, col. 6, lines 15-21).

Neither **Garrison** nor **Yoshimoto** explicitly teaches an apparatus wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network.

De Capitani di Vimercati et al., however, teaches an apparatus wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the three references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **Yoshimoto**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network, since it is necessary to protect all information transferred over the global communication network (see **Capitani di Vimercati et al.**, page 93, col. 2, second to last paragraph).

20. Regarding claim 11, **Garrison** teaches a method of utilizing a user terminal having a user with a user identifier located at a site to securely access a remote database management system having a database via a publicly accessible digital data communication network as claimed, comprising:

a) signing on to said terminal by said user utilizing said user identifier (see col. 2, line 64 through col. 3, line 2, disclosing that the client transmits a password to the client to identify the user of the client system, meaning that the user has necessarily signed on to the client system utilizing a user identifier);

b) transmitting a service request requiring secure access to said database from said terminal (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);

c) receiving said service request by said remote database management system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);

d) determining a security profile (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);

e) comparing said security profile with said service request (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37); and

f) honoring said service request if and only if said service request corresponds to said security profile (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

Garrison does not explicitly teach a method wherein the security profile is site-specific.

Yoshimoto, however, teaches a method wherein the security profile is site-specific (see Abstract; see also col. 1, line 63 through col. 2, line 6).

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a site-specific security profile, since this would allow the level of access granted to a user to be based in part on the security of the specific terminal or location from which the access request is generated, thus inhibiting illegitimate access from a terminal having poor security (see **Yoshimoto**, col. 6, lines 15-21).

Neither **Garrison** nor **Yoshimoto** explicitly teaches a method wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network.

De Capitani di Vimercati et al., however, teaches a method wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2

Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the three references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **Yoshimoto**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network, since it is necessary to protect all information transferred over the global communication network (see **Capitani di Vimercati et al.**, page 93, col. 2, second to last paragraph).

21. Regarding claim 16, **Garrison** teaches an apparatus as claimed, comprising:

a) means located at a site for permitting a user having a user identifier to interact with a database responsively coupled via a publicly accessible digital data communication network (see col. 4, lines 1-32);

b) means responsively coupled to said permitting means via said publicly accessible digital data communication network for offering data processing services involving access to said database in response to said service request (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37); and

c) means responsively coupled to said offering means for preventing said offering means from offering said data processing services to said user in response to said service

request unless said site corresponds to a security profile wherein said security profile permits access to said database (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

Garrison does not explicitly teach an apparatus wherein the security profile is site-specific.

Yoshimoto, however, teaches an apparatus wherein the security profile is site-specific (see Abstract; see also col. 1, line 63 through col. 2, line 6).

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a site-specific security profile, since this would allow the level of access granted to a user to be based in part on the security of the specific terminal or location from which the access request is generated, thus inhibiting illegitimate access from a terminal having poor security (see **Yoshimoto**, col. 6, lines 15-21).

Neither **Garrison** nor **Yoshimoto** explicitly teaches an apparatus wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network.

De Capitani di Vimercati et al., however, teaches an apparatus wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2

Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the three references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **Yoshimoto**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network, since it is necessary to protect all information transferred over the global communication network (see **Capitani di Vimercati et al.**, page 93, col. 2, second to last paragraph).

22. Regarding claim 2, **Garrison** additionally teaches a data processing environment wherein a security profile is generated by said data management system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

23. Regarding claims 3, 8, 12, 13 and 18, **Garrison** additionally teaches an improvement, method and apparatus further comprising a portion of a service request whereby said database management system receives an identifier corresponding to said particular site (see discussion of predefined password at col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

24. Regarding claims 4, 14 and 17, **Garrison** additionally teaches an improvement, method and apparatus wherein said publicly accessible digital data communication network further comprises the Internet (see col. 4, lines 1-32).

25. Regarding claim 7, **Garrison** additionally teaches an apparatus wherein said terminal accesses said data entity by transferring a service request to said system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

26. Claims 5, 9, 10, 15, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **Yoshimoto** (U.S. Patent 6,237,023) in view of **De Capitani di Vimercati et al.** ("Access Control in Federated Systems") as applied to claims 1-4, 6-8, 11-14 and 16-18 above, and further in view of **Unisys** ("UNISYS CSG MarketPlace – The Mapper System").

27. Regarding claims 5, 9, 15 and 19, **Garrison, Yoshimoto** and **De Capitani di Vimercati et al.** teach an improvement to a data processing environment, method and apparatus substantially as claimed.

None of **Garrison, Yoshimoto** nor **De Capitani di Vimercati et al.** explicitly teaches the improvement, method and apparatus wherein said database management system is MAPPER.

However, **Unisys** teaches the database management system MAPPER (see entire document).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER contains many key features that make its use advantageous for users (see **Unisys**, key features under MAPPER Overview, page 3).

28. Regarding claim 10, **Garrison** additionally teaches an apparatus wherein said publicly accessible digital data communication network further comprises the World Wide Web (see col. 4, lines 1-32).

29. Regarding claim 20, **Garrison** additionally teaches an apparatus wherein said permitting means further comprises an industry standard personal computer (see col. 4, lines 1-60).

30. Claims 5, 9, 10, 15, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **Yoshimoto** (U.S. Patent 6,237,023) in view of **De Capitani di Vimercati et al.** ("Access Control in Federated Systems") as applied to claims 1-4, 6-8, 11-14 and 16-18 above, and further in view of **Unisys** ("Why Do I Need Cool ICE?").

31. Regarding claims 5, 9, 15 and 19, **Garrison, Yoshimoto** and **De Capitani di Vimercati et al.** teach an improvement to a data processing environment, method and apparatus substantially as claimed.

None of **Garrison, Yoshimoto** nor **De Capitani di Vimercati et al.** explicitly teaches the improvement, method and apparatus wherein said database management system is MAPPER.

However, **Unisys** teaches a system wherein the database management system used is MAPPER (see page 3, second paragraph).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER has been tuned for reliability, scalability, and high performance, and furthermore, since the technology has been used for years by thousands of users for many different kinds of applications, and since it has gained a reputation for performing well for everything from small data analysis applications to huge transaction systems, and since its reliability is exemplary (see **Unisys**, page 3, second paragraph).

32. Regarding claim 10, **Garrison** additionally teaches an apparatus wherein said publicly accessible digital data communication network further comprises the World Wide Web (see col. 4, lines 1-32).

33. Regarding claim 20, **Garrison** additionally teaches an apparatus wherein said permitting means further comprises an industry standard personal computer (see col. 4, lines 1-60).

Response to Arguments

34. Applicant's arguments filed 9 February 2004 have been fully considered but they are not persuasive.

35. In response to the Applicants' arguments regarding the objections to the specification, the examiner has withdrawn these objections.

However, in light of these arguments, the examiner requests clarification from the Applicants as to the advantage of using the claimed system.

In the preliminary amendment, the Applicants state on page 9, second paragraph of the Remarks that "those of skill in the art will readily appreciate that a user-id and a password are just numbers." The invention prevents hackers from accessing secure data because a user-specific user-id is never transmitted over the Internet. However, *some* identifier is transmitted, be it 'site specific data' (specification, page 7, lines 16-20, wherein site-specific data is transmitted to the server and there converted to a valid user-id and password) or a user-id/password that corresponds to the site (specification, page 7, lines 12-14, wherein site-specific data is converted to a user-id and password at the site, and then transmitted to the server).

The question, then, is if the potential exists for a hacker to intercept a user-specific user-id/password, and use it to surreptitiously access secure data, what is there to prevent this same hacker from intercepting the site-specific user-id/password or site-specific data, and using this information in exactly the same manner? As the Applicants noted, user-ids and passwords are nothing more than numbers, so what makes the transmission of user-specific 'numbers' any different from site-specific 'numbers', when either has the potential to provide a user (or a hacker) access to secure data?

The Applicants themselves admit in the Remarks at page 12, second to last paragraph, that "A UserID/Password is a number. The number is exactly the same whether assigned to uniquely identify a particular user or generated by the system to uniquely identify a physical site. There is no difference."

36. The examiner does not find the Applicants' arguments regarding the claim rejections under 35 U.S.C. § 112, first paragraph persuasive.

The claims cite the fact that secure data can be accessed without transmitting a user-id. This is inconsistent with the teaching of the specification at pages 33-34, where it is taught that if a security profile is not associated with a requested service request, the service request is carried out, but if a security profile is associated with a requested service request, then

> "**service handler 332 requests the user to provide a user-id via** path 330, Cool ICE object 322, and **world wide web path** 312. **Service handler 332 awaits a response via world wide web** path 308, Cool ICE object 322 and path 326. **Service handler 332 compares the user-id received** to the security profile stored with the command language script. If the user matches the security profile, access is granted and service handler 322 proceeds as described above."

The plain implication is that if secure data is requested (assuming that an associated security profile indicates the presence of secure data), then **the user** is requested to provide a user-id, and this user-id is transmitted to the server via the world wide web. This is contrary to the claim language whereby access to secure data is granted without the transmission of user identification information over a publicly accessible digital data communications network.

The Applicants argue that in this case, the service handler may receive a site specific UserID/Password rather than a user-specific UserID/Password (Remarks, page 14, first paragraph). However, if **the user** is requested to provide a user-id, then the user-id provided by the user is obviously user-specific.

37. The examiner does not find the Applicants' arguments regarding the rejections of the claims based on the **De Capitani di Vimercati et al.** reference persuasive.

The Applicants have added the limitation that the requested data is secure data. The examiner respectfully responds that the fact that the data at issue in the **De Capitani di Vimercati et al.** reference can only be accessed after validating the authorization of the entity requesting the data (whether that entity's authorization be validated on a user-by-user basis, or on a site-by-site basis) makes explicit the fact that the data is secure data. Were the data not 'secure', then there would be no access control nor authentication required at all.

Conclusion

38. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Calo et al. (U.S. Patent 4,805,134) teaches a system fir distributed access to information, whereby users have registered profiles at each operations node and whereby each profile is identified by a node-specific identifier.

Wade et al. (U.S. Patent 5,552,776) teaches a system for accessing distributed information whereby the system has a password table comprising passwords for authorized site ids.

Icken et al. (U.S. Patent 6,662,181) teaches a system for distributed access to information whereby access may be restricted based on the location of the user and the information.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luke S. Wassum whose telephone number is 703-305-5706. The examiner can normally be reached on Monday-Friday 8:30-5:30, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John E. Breene can be reached on 703-305-9790. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

In addition, INFORMAL or DRAFT communications may be faxed directly to the examiner at 703-746-5658.

Customer Service for Tech Center 2100 can be reached during regular business hours at (703) 306-5631, or fax (703) 746-7240.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Luke S. Wassum
Art Unit 2177

lsw
17 March 2004